*Salud, Ciencia y Tecnología*. 2022; 2(S2):244
doi: 10.56294/saludcyt2022244

**ORIGINAL**

# DoS Attack Detection Mechanism in Wireless Sensor Networks

## Mecanismo de detección de ataques DoS en redes de sensores inalámbricas

Himani Sharma[1], Basheer Shajahan[1], Rajesh Elangovan[1], Manikandan Thirumalaisamy[1]

[1]Galgotias University. School of Computer Science and Engineering. Uttar Pradesh, India.

**Cite as:** Sharma H, Shajahan B, Elangovan R, Thirumalaisamy M. DoS Attack Detection Mechanism in Wireless Sensor Networks. Salud Cienc. Tecnol. 2022; 2(S2):244. https://doi.org/10.56294/saludcyt2022244

**Submitted:** 07-11-2022 **Revised:** 20-12-2022 **Accepted:** 26-12-2022 **Published:** 31-12-2022

**Editor:** Fasi Ahamad Shaik

**ABSTRACT**

Wireless sensor networks (WSNs) are not like traditional networks in terms of their characteristics. Unlike WSN, in classic networks, networking mechanisms have decision-making power with reference to the management of an incoming packet only based on its internet protocol (IP) destination address. Assailant nodes can activate a denial of service (DoS) attack after entering the network. This research work focuses on tracing these collusive nodes by applying a trust-based scheme. The trust-based scheme includes measuring the degree of trust among all nodes. Nodes with minimum trust are designated as malicious nodes. Trust is measured based on the overall packets transferred during the time slot allotted. The node forwarding maximal packets and exploiting minimal assists will be tagged as malicious. The nascent architecture was deployed in NS2, and the outcomes were analysed based on particular performance metrics. To calculate trust, the overall packets forwarded by nodes in the allotted slot were considered. The node that transmits the largest number of packets and uses negligible assets was declared a vindictive node. This task implementation presents the approach in the NS2 software and analyses the results based on certain metrics.

**Keywords:** DOS; Trust Mechanism; Threshold Value; WSN.

**RESUMEN**

Las redes inalámbricas de sensores (WSN) no se parecen a las redes tradicionales en cuanto a sus características. A diferencia de las WSN, en las redes clásicas los mecanismos de red tienen poder de decisión en lo que se refiere a la gestión de un paquete entrante únicamente en función de su dirección de destino del protocolo de Internet (IP). Los nodos agresores pueden activar un ataque de denegación de servicio (DoS) tras entrar en la red. Este trabajo de investigación se centra en rastrear estos nodos colusorios aplicando un esquema basado en la confianza. El esquema basado en la confianza incluye la medición del grado de confianza entre todos los nodos. Los nodos con un mínimo de confianza se designan como nodos maliciosos. La confianza se mide en función del total de paquetes transferidos durante el intervalo de tiempo asignado. El nodo que reenvíe el máximo de paquetes y aproveche las mínimas asistencias será etiquetado como malicioso. La arquitectura naciente se desplegó en NS2 y los resultados se analizaron en función de determinadas métricas de rendimiento. Para calcular la confianza, se tuvo en cuenta el total de paquetes reenviados por los nodos en la franja horaria asignada. El nodo que transmite el mayor número de paquetes y utiliza activos insignificantes fue declarado nodo reivindicativo. La implementación de esta tarea presenta el enfoque en el software NS2 y analiza los resultados en función de determinadas métricas.

**Palabras clave:** DOS; Mecanismo de Confianza; Valor Umbral; WSN.

## INTRODUCTION

WSN is a decentralized network type that involves numerous arbitrarily dissipated sensing devices. Cheap sensing devices increase the reasonability of WSNs for miscellaneous applications like disaster area observation, climate monitoring, congestion handling, and medical services, among other areas. These devices have the potential to sense physical or climate properties at different locales, for example, pollutants, the environment, acoustics, earthquakes, gravity, and so forth.[1]

The properties monitored are transferred to the base station (BS) which, after gathering all information, passes it on to the client over the internet. The enormous number of nodes are dispersed in an open and threatening environment to get information from the region under surveillance. This operation needs a coordinated effort among the gigantic number of sensing devices for monitoring the target area. Since the limit of a node is confined to the observation zone and communication range the nodes are left with no choice except to help out one another in the network.

In this approach, the coordinated effort of the nodes is critical for increasing wireless sensor network productivity. WSNs can be harmed by malicious acts. Because of such vengeful attacks, the majority of energy is spent on water.[2] Therefore, developing an effective mechanism is necessary to distinguish vindictive assault, adjust the use of energy, and prolong the network service duration. Assailants activate a wide array of assaults on WSNs, for example, sinkhole, Sybil, wormhole, etc. WSN assaults are divided into two categories: external assaults and internal assaults. An assailant performs an external attack by injecting an external entity into the network. The objective of this assault is to ruin the entire functioning of the network. In an internal attack, the attacker either targets the domain or enters the network through a colluded sensor node.

A DoS Attack is usually described as the malevolent endeavor by one or a bunch of individuals to deny service to network users. DoS attacks launched on the network either harm or prevent the smooth operation of the network. The most common way to launch this attack is to overload the target system with requests in order to avoid or prevent response to legitimate traffic. Consequently, the system or service turns out to be inaccessible to the user.[3]

This attack is mostly not launched to get unauthorized access but just to create a mess. This attack interrupts the services of the network.[4] Moreover, this attack may damage network elements physically by using scarce, restricted, or non-renewable resources. Sometimes, it causes destruction and changes the formation of information. The underlying set-up of a DoS attack in WSN is a feature in figure 1.

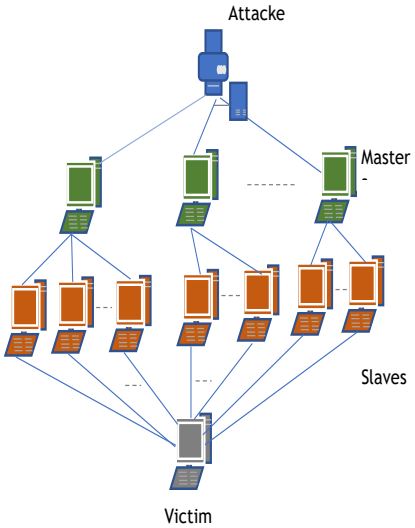


**Figure 1**: DoS attack in WSN.

Figure 1 shows the DoS attack scenario, comprising three different stages and four different elements. In the initial stage, the intruder takes a significant amount of time to generate a large number of compromised machines, known as masters or handlers. These elements hire and manage other machines in the attacking group. The master army is generally created automatically via continuous scanning of search machines with security gaps. Additional compromised machines are infused into the attacking group by malicious codes placed by the intruder on this group of masters.[5]

The masters and attackers have direct and indirect control of slave machines. The next stage starts by injecting an adequate number of devices into the infected group. This infected group is known as a "botnet." The assailant transmits all critical data and provides instructions to the group of masters, which pass on

this data further to all slaves and prepare them to activate an assault. In the last stage, the assailant gives instructions to its slaves regarding the launching of attacks, after which they launch an attack on the victim in a dispersed manner and flood the system of the victim. In these attacks, the attacker generally makes use of spoofed IP addresses to hide the actual identity of the adversaries.

Denial of attack is described as an event that diminishes or attempts to alleviate the capacity of a network while carrying out its expected function. Several standard methods are present in the literature for resisting DoS intrusions, even though it is an open issue to design a generic defense system against these attacks in the greater context.

Additionally, the high computational overhead is necessitated by almost all of the defense mechanisms. Thus, they are not adequately demonstrated for resource-constrained wireless sensor networks.[6] Various efforts are made to recognize several categories of these attacks. Moreover, strategies are also designed by researchers for defending against these attacks. There are some major kinds of Denial of attacks present in dissimilar layers of networks, which are described as:

a. Attacks on the Physical layer: It is responsible to select the frequency, generating carrier frequency, detecting the signal, and encrypting the data. The ndtes in radio networks are carried out in unfriendly or doubtful surroundings in which physical access is given to the attacker. Two kinds of assaults available at this layer are described as follows:

i. Jamming: It's a type of attack that interferes with the radio frequencies that are used to establish communication between nodes in a WSN. A jamming source is dominant enough for interrupting the whole network. An adversary is capable of upsetting the message sharing within the whole network even with the least significant jamming causes. For this purpose, the jamming sources are distributed intentionally. Even intermittent jamming is demonstrated as detrimental because of the time sensitivity of the message communication in these networks.

ii. Tampering: WSNs are deployed in outdoor environments in general. The nodes in WSNs have a high vulnerability to physical attacks because of their unattended and distributed nature (7). Irreversible damage can occur to the nodes with the physical attacks. The adversary has the potential for extracting the cryptographic keys from the seized node, tamper with its electric circuit, modifying the programming codes, or even replacing it with a vindictive device.

b. Attacks on Link layer: It is accountable for the multiplexing of the sequence of data, detecting the data frame, and controlling the medium access and error. The collisions are generated intentionally but the resource is exhausted and unfairness has occurred in allocation during the occurrence of attacks in the link layer. A collision is generated at the time of transmission on the same frequency by two nodes at the same time. This collision of packets leads to discarding those packets and requires retransmission. The collisions may generate specific packets in terms of ACK control messages with an adversary. A possible outcome of these kinds of collisions is an exponentially expensive back-off (8). This adversary is capable of violating the transmission protocol and incessantly transmitting the messages to produce crashes. An attacker may carry out repeated collisions for generating resource exhaustion. To illustrate, a naïve link layer execution is constantly attempting the retransmission of the corrupted packets. The exhaustion of energy levels of the nodes takes place speedily if these retransmissions are not detected earlier. Unreasonableness is a feeble kind of DoS assault. The above link layer attacks are employed by an assailant to cause unfairness intermittently. The realistic applications which run on other nodes are degraded via adversary. For this, their frame transmissions are interrupted from time to time in that situation.

c. Attacks on the network layer: The primary responsibility of the network layer in a WSN is data routing. WSNs are vulnerable to a variety of attacks, including bogus routing information, Sybil, SPF (Selective packet forwarding), Wormhole, Blackhole, Hello flood, sinkhole, among others. A few of them are elaborated as follows:

i. Blackhole and Gray hole: A colluded node activates this attack by promoting fake messages about having the most optimal route (for example, direct route or steady route) to the destination at the time of route discovery, or during route updating. A colliding node's goal might be to sabotage the route discovery process or to sabotage data packet delivery to the relevant node at the destination. This technique is also known as the grey hole attack, since the colluding node unpredictably drops data packets, making it even more difficult to detect.

ii. Hello flood: The majority of protocols using hello packets believe in the theory that obtaining such a packet means that the forwarder is within the radius of the receiver. An assailant can employ a transmitter with high energy to deceive multiple nodes and trick them into believing they are in its vicinity (9). Next, the attacking node misleadingly establishes a direct route to the sink, and all nodes that receive the hello packet try to pass it on to the attacking node. Nevertheless, these nodes do not fall into the attacker's coverage area.

iii. Sinkhole: An assailant activates a sinkhole attack by making a colluded node more striking to its surrounding nodes by falsifying the info of routing. As a result, nodes in the vicinity choose the colluding node as their next-hop node and relay their data to it. Because all traffic from a bigger part of the network will pass from the colluding node, this technique substantially facilitates selective forwarding.

d. Attacks on the Transport layer: Flooding and de-synchronization are the most common attack types at the transport layer. Both of these attack types are elaborated as follows:
   i. Flooding: Flooding causes a protocol susceptible to the wastage of memory, whenever it tries to uphold state on any end of a link. When a protocol is needed to keep state on both ends of a connection, it is prone to flooding, which causes memory exhaustion. An attacker can iteratively request additional connections until all resources required for each link have been exhausted or the maximum threshold has been achieved (10). In any scenario, more legitimate requests will be turned down.
   ii. Desynchronization: Desynchronization is the state of the dissolution of an existent link. An assailant could repetitively send fake messages to the final host, thereby requesting the host to retransmit the lost frame. Through appropriate scheduling, an assailant can scale down or even preclude the potential of hosts at the destination to share data efficiently, allowing them to waste energy trying to remove errors that don't exist.

## LITERATURE REVIEW

Thi-Thu-Huong Le et al.[11] suggested a novel technique for predicting DoS attacks in WSNs. The RF (Random Forest) classification algorithm was adopted for detecting the kind of DoS attacks such as those on the WSN-DS dataset.

The experimental results depicted that the suggested technique performed more effectively as compared to other techniques in WSN. The suggested technique was capable of obtaining the F1-score 99 % for detecting Blackhole attacks, 96 % for Flooding attacks, 98 % for Grayhole attacks, 100 % for normal attacks, and 96 % for TDMA (Scheduling) attacks. Their future work would focus on implementing the suggested technique on other WSN datasets and predicting DoS attacks as well as other attacks.

Chen Lyu et al.[12] presented the SelGOR (Selected Authentication based Geographic Opportunistic Routing) method for preventing DoS attacks and making WSNs more authentic and dependable. The SSI (statistic state information) based trust model is applied to increase data transmission efficacy and is investigated using the SSI of wireless networks. This work developed an entropy-based selective authentication system that ensured data integrity while simultaneously reducing computation costs and isolating DoS attackers. Moreover, a distributed cooperative verification method was put forward for enhancing the process of isolating the attackers.

The forwarding of duplicate data and the verification of redundant signatures were avoided by the opportunistic routing in this algorithm. The output of the simulation demonstrated that the introduced algorithm is very effective for transmitting the data reliably and authentically and consuming a computational cost of only 50 % in comparison with other techniques.

Puja Rani et al.[13] formulated a trust-based security technique against DoS attacks in WSNs. DoS attackers focused their efforts on flooding the network with duplicate packets. The goal of using this approach was to identify the impact of a DoS (Denial of Service) attack on the traffic and classify the nodes. Collaborative and data trust are detected using the Trust-Based method.

The data trust was calculated using RSS (Received Signal Strength) and node energy. Diverse parameters including routing load, throughput, and others were considered to quantify the efficacy of the network. The simulation results indicated the supremacy of the formulated technique over the traditional technique.

Quincozes et al.[14] described that the major goal was to evaluate the efficacy of the ML (Machine Learning) techniques for detecting various DoS (Denial of Service) attacks WSNs. WSN-DS dataset was applied to stimulate the presented techniques concerning accuracy and speed. The results showed that the J48 algorithm was an effective technique for identifying the gray-hole, and black holes. Furthermore, the flooding attack was detected using the RT (Random Tree) technique. The J48 technique performed more quickly and was utilized for an average of 0,54 microseconds in processing.

Mousa Al-Akhras et al.[15] projected an IDS (Intrusion Detection System) for detecting DoS attacks on a specialized WSNs dataset. The DT (Decision Tree) and ANN (Artificial Neural Network) algorithms were presented for detecting the signature of DoS attackers. This system focused on selecting attributes from the dataset. This resulted in diminishing the time required for learning the signature of the attacker and enhancing the speed at detecting the attack. The outcomes exhibited that the applicability of both the algorithms in case of utilization of relevant attributes and DT performed better in contrast to others. The DT algorithm offered an accuracy of 99,83 %, a TP (True Positive) of 0,998, and a FP (False Positive) of 0,014. On the other hand, the ANN algorithm yielded an accuracy of 99,76 %, a TP of 0,998, and a FP of 0,004.

Al-issa et al.[16] emphasized developing a system for WSN (Wireless Sensor Network) to detect DoS (Denial of Service) attacks with optimized cost, complexity, and energy-saving utilization. The dataset was generated for classifying four types of DoS attacks: Black-hole, Gray-hole, Scheduling, and Flooding. This system implemented DT (Decision Tree) and SVM (Support Vector Machine) and used them for testing the efficiency to detect the DoS attack on the WSN dataset. The experimental outcomes confirmed that the DT offered a higher TPR (true positive rate) of 99,86 % and the lowest FPR (false positive rate) of 0,05 % in comparison with the SVM.

Premkumar et al.[17] researched DLDM (Deep Learning-based Defence Mechanism) as a unique lightweight approach for identifying and isolating DoS threats in DFP (Data Forwarding Phase). This technique had the potential to detect the DoS attacks namely exhaustion, jamming, homing, and flooding successfully. The experiments were performed for isolating the adversaries and evaluating the resiliency of the investigated technique against DoS attacks. The experimental results revealed that the investigated technique offered higher DR (detection rate), PDR (packet delivery ratio), accuracy, and throughput. Moreover, the investigated technique was applicable to mitigate the energy usage and FAR (false alarm rate).

Xie Jinhui et al.[18] established a node energy consumption analysis method for generating IDS (Intrusion Detection System) based on the trust of energy consumed via node for enhancing the rate to detect the hybrid DoS attack in WSNs. Based on an energy consumption forecast method, a power series correlation check was given. The experimental results showed that the developed technique was successful in raising the success rate for detecting the malicious node, prolonging the network duration, and limiting the effect of a hybrid Denial of Service attack on packets transferring over the network when a hybrid DoS occurred in the network.

Chengyi Yang et al.[19] intended an energy-aware mechanism based on spectrum detection in WSN (Wireless Sensor Network) applications to save the cost of gathering the data and computing the potential for detecting the DDoS (Distributed Denial of Service) attack without any collection of a huge number of traffic attributes and training of a large-scale DL (deep learning) model. When the busy channel was detected, the topology of WSN (Wireless Sensor Network) was utilized to estimate the scope of the DDoS attack. The simulation results validated that the intended mechanism provided higher efficiency and accuracy, and was appropriate to meet the demands of low load and high security of WSN.

Kurniawan et al.[20] discussed how DoS attacks focused on preventing authentic users from accessing resources, reducing the available resources until the network resources became overburdened. Thus, the DoS attacks needed to be detected and mitigated. A signature-based IDS (Intrusion Detection System) was used to identify and mitigate DoS assaults, using a blocking mechanism displayed on the attack node. All packets coming from the attacker were stopped as a result of this. This technique was utilized after detecting the DoS attack using the exploited system. The results revealed that the presented technique was capable of mitigating the DoS attacks.

## METHODS

The incepted network has the following steps:

### *3.1. Pre-processing and Network deployment*

The number of nodes in a WSN is fixed. A malicious node is the one that initiates a DDoS attack. Several techniques for detecting malicious nodes have been proposed in the past year. The threshold value is the foundation of the methods used in this study. This effort will use a novel way to determine the data rate threshold value. The formula for determining the malicious node recognition threshold data rates is given below in equation 1.

$$P = Pb * max\_p \qquad (1)$$

The "average" data rate used in the experiment is represented by a variable named "average." The average used here is 1 packet every 0.5 seconds of data. The letter "min" stands for the lower limit of the data rate, while "max" stands for the higher limit. The threshold data rate is computed by multiplying Pb by the higher limit value. Figure 2 illustrates the flow chart of the suggested scheme.

*Malicious nodes Detection*

Nodes are arbitrarily scattered in a given location. To trace attacking nodes, the introduced scheme applies a single hop delay. Actual nodes broadcast many packets, and IDS nodes are those that fill the packet with the maximum number of nodes. These IDS nodes are bad nodes that disrupt the appropriate management of WSN. There is a threshold limit, and if network throughput goes beyond that limit, then a new strategy is applied where every node monitors its adjacent node; this is called the monitor mode strategy. If a node continues to accept or transmit data packets over the threshold limit, it is labeled as malicious. If a malicious node receives a control packet, the node is labeled as corrupted.

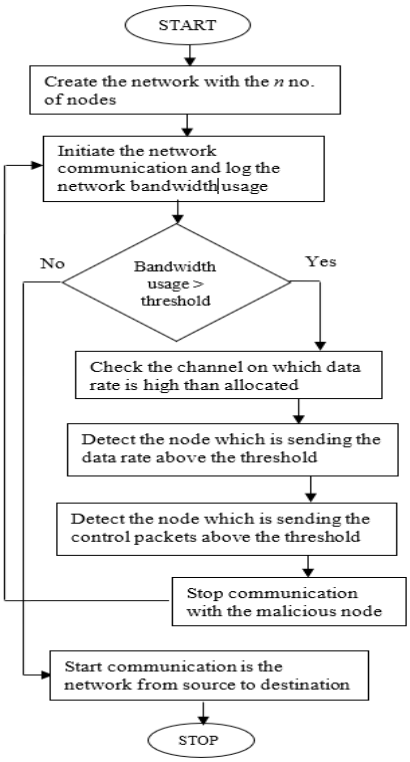


**Figure 2.** Proposed Framework

*Exclusion of Malicious nodes*

The network data rate is already being monitored, and any node that exceeds the threshold limit is labeled as malevolent. For identifying and removing the malicious node, the source node sends the warning packet to each node. After receiving the warning packet, the legitimate nodes will remove the malicious node from the routing table entries.To detect malicious nodes, the approach chosen corresponds to the complexity and includes several congested values. This step includes removing corrupted nodes from the routing path of the network. A broadcast signal is sent to all network nodes by an adversary node. The node that receives this signal adopts multipath routing to prevent communication with other nodes. Nodes that are incapable of validating their ID are abolished from the network.

## RESULT AND DISCUSSION

A trust-based technique for identifying malicious nodes was provided by the threshold-based approach. The Network Simulator 2 was used for implementing the framework created in this study. Table 1 features the simulation metrics as described.

**Table 1**. Simulation Metrics

| S. No. | Parameters | Values |
|---|---|---|
| 1 | Nodes Number | 38 |
| 2 | Queue Size | 50 |
| 3 | Propagation Model | Two-Ray |
| 4 | Antenna type | Omni-Directional |
| 5 | Queue type | Priority-Queue |
| 6 | Area | 800800 |
| 7 | Traffic Type | CBR |

**Throughput:** It is a performance measurement used to check performance. The throughput parameter counts the number of packets that are successful in reaching their destination in a unit of time. The throughput may be evaluated as per the following equation 2.

https://doi.org/10.56294/saludcyt2022244

$$Throughput = \frac{Total\ received\ data\ packets}{Total\ sent\ data\ packets} * Time \qquad (2)$$

**Delay**: A network delay demonstrates that a data bit has been expended to move from one given node or endpoint in the network to another. The network delay can be measured using the given equation 3.

$$Delay = \frac{\sum(Time\ Received - Time\ Sent)}{Total\ Data\ Packets\ Received} \qquad (3)$$

**CMO (Control Message Overhead):** It denotes actual processing time, including node discovery, network latency, memory, bandwidth, or other resources needed to complete a task. The CMO is described in equation 4.

*CMO = Number control message transmitted * Time* (4)

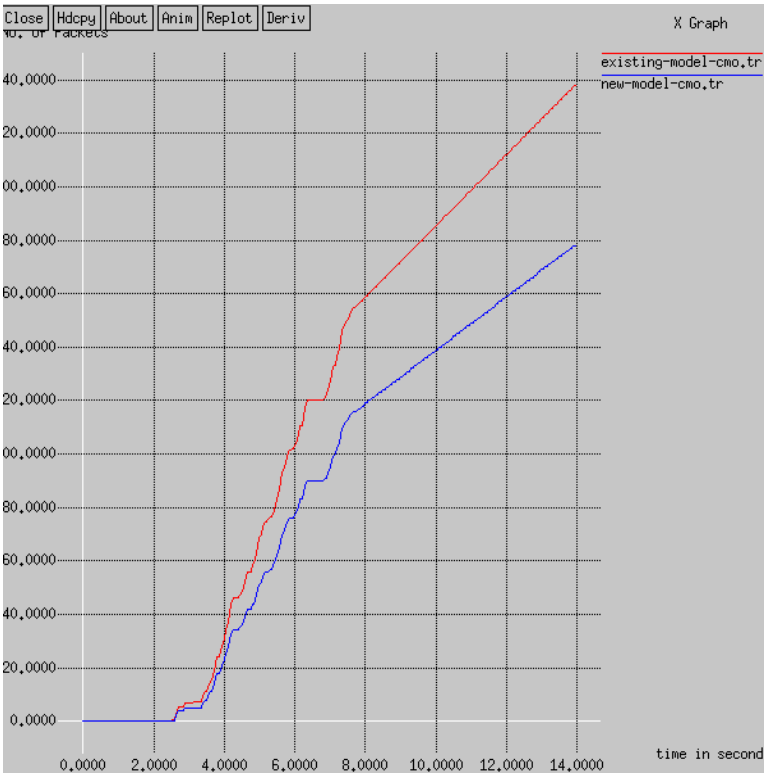


**Figure 3.** Control Message Overhead Comparison

**Table 2.** Control Message Overhead

| S. No. | Time | Existing Model | Proposed Model |
|---|---|---|---|
| 1 | 4 seconds | 35 Packets | 25 Packets |
| 2 | 10 seconds | 185 Packets | 140 Packets |
| 3 | 14 seconds | 238 Packets | 178 Packets |

Table 2 illustrates the control message overhead. Figure 3 exhibits a comparative analysis of two scenarios in terms of control message overhead. The two scenarios include the attack scenario and the nascent scheme. As per the results, the SHIELD mechanism is the current approach to isolate DoS intrusions. The new scheme is a trust-based methodology to counter DoS intrusions.

Figure 4 exhibits a comparative analysis of two scenarios in terms of delay. The two scenarios include the attack scenario and the nascent scheme. As per the results, the SHIELD mechanism is the current approach to isolate DoS intrusions. The new scheme is a trust-based methodology to counter DoS intrusions. The new approach is better in terms of delay than the existing approach. And from Table 3, we can see that the delay has been reduced to 17 %.

Figure 5 exhibits a comparative analysis of two scenarios in terms of control message overhead. The two scenarios include the attack scenario and the nascent scheme. The SHIELD mechanism is the current approach to isolate DoS intrusions. The new scheme is a trust-based methodology to counter DoS intrusions. As a result,

the nascent scheme provides better throughput than the old scheme. And from Table 4, we can see that the Overall Throughput has increased to 12 %.

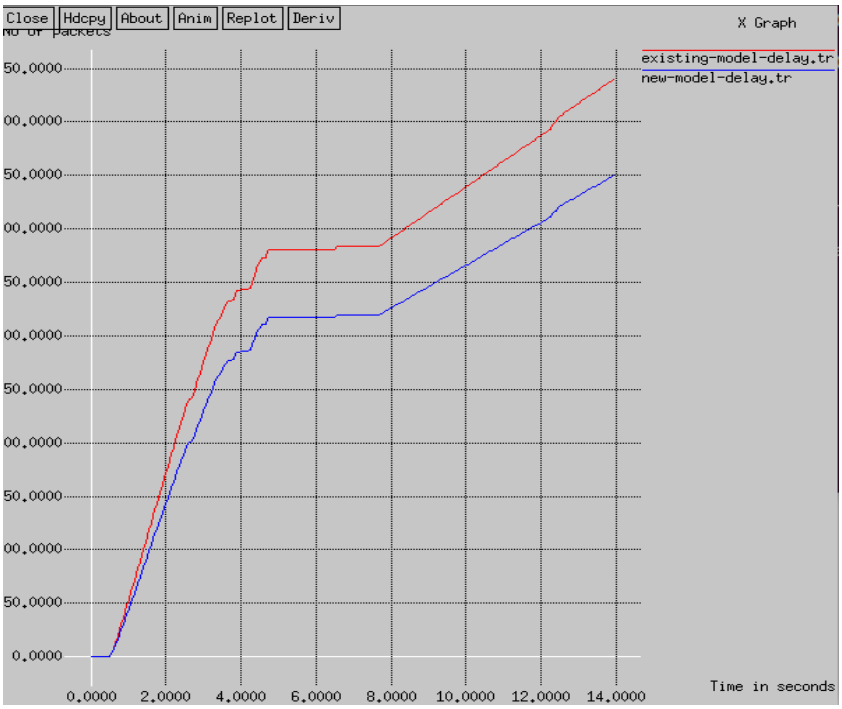


**Figure 4.** Delay Comparison

**Table 3**. Delay Analysis

| S. No | Time | Existing Model | Proposed Model |
|---|---|---|---|
| 1 | 4 Seconds | 345 Packets | 280 Packets |
| 2 | 10 Seconds | 440 Packets | 370 Packets |
| 3 | 14 Seconds | 540 Packets | 450 Packets |

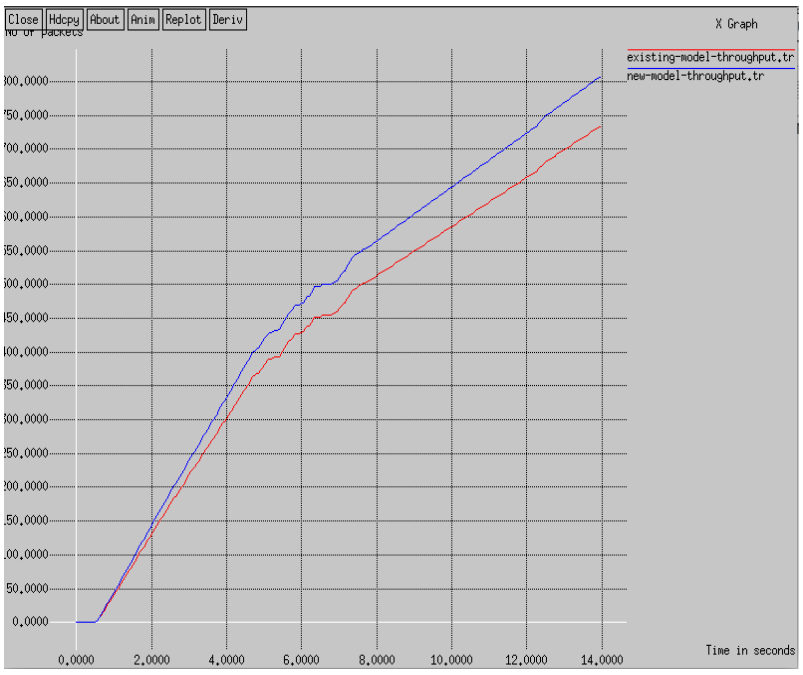


**Figure 5.** Throughput Comparisons

https://doi.org/10.56294/saludcyt2022244

**Table 4.** Throughput Analysis

| S. No. | Time | Existing Model | Proposed Model |
|---|---|---|---|
| 1 | 4 Seconds | 300 packets | 350 packets |
| 2 | 10 Seconds | 580 Packets | 645 Packets |
| 3 | 14 Seconds | 735 Packets | 810 Packets |

## CONCLUSION

The goal of this research is to reduce DoS attacks on wireless sensor networks. To avoid DoS attacks on the network and identify rogue nodes, this solution implemented trust-based mechanisms. The trust-based approach makes the most of the network resources. The trust-based strategy is based on the packet forwarding threshold value. The adversary tag is given to the node that can transport the most packets while using the fewest resources. The suggested new architecture is built in NS-2, and the results were tested against throughput, latency, and CMO criteria. The proposed model shows that throughput is increased up to 12 %. The delay is reduced up to 17 %. The CMO is reduced to 10 %. The overall results have improved by 10 to 15 %.

## REFERENCES

1. Chen H, Meng C, Shan Z, Fu Z, Bhargava BK. A Novel Low-Rate Denial of Service Attack Detection Approach in ZigBee Wireless Sensor Network by Combining Hilbert-Huang Transformation and Trust Evaluation. IEEE Access. 2019; 7:32853-66.

2. Kaur R, Sandhu JK. A Study on Security Attacks in Wireless Sensor Network. In: Proceedings of the 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE); 2021. p. 850-5.

3. Jilani SA, Koner C, Nandi S. Security in Wireless Sensor Networks: Attacks and Evasion. In: Proceedings of the 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA); 2020. p. 1-5.

4. Moorthy RH, Bangera V, Amrin Z, Avinash NJ, Rao NSK. WSN in Defence Field: A Security Overview. In: Proceedings of the 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC); 2020. p. 258-64.

5. Gunduz S, Arslan B, Demirci M. A Review of Machine Learning Solutions to Denial-of-Services Attacks in Wireless Sensor Networks. In: Proceedings of the 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA); 2015.

6. Mansouri D, Mokddad L, Ben-othman J, Ioualalen M. Preventing Denial of Service attacks in Wireless Sensor Networks. In: Proceedings of the 2015 IEEE International Conference on Communications (ICC); 2015.

7. Yang Z. Attack and Defense Game Strategy of Wireless Sensor Networks under Multiple Attacks. In: Proceedings of the 2019 Chinese Control Conference (CCC); 2019. p. 6349-56.

8. R D, Chinnaiyan R. Reliable Constrained Application Protocol to Sense and Avoid attacks in WSN for IoT Devices. In: Proceedings of the 2019 International Conference on Communication and Electronics Systems (ICCES); 2019. p. 1898-1901.

9. Pruthi V, Mittal K, Sharma N, Kaushik I. Network Layers Threats & its Countermeasures in WSNs. In: Proceedings of the 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS); 2019. p. 156-63.

10. Bharti D, Nainta N, Monga H. Performance Analysis of Wireless Sensor Networks Under Adverse Scenario of Attack. In: Proceedings of the 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN); 2019. p. 826-8.

11. Le T-T-H, Park T, Cho D, Kim H. An Effective Classification for DoS Attacks in Wireless Sensor Networks. 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN); 2018. p. 689-692.

12. Lyu C, Zhang X, Liu Z, Chi C-H. Selective Authentication Based Geographic Opportunistic Routing in

Wireless Sensor Networks for Internet of Things Against DoS Attacks. IEEE Access. 2019;7:31068-31082.

13. Rani P, Gupta NK. Composite Trust for Secure Routing Strategy through Energy based Clustering in WSN. 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT); 2021. p. 1-6.

14. Quincozes SE, Kazienko JF. Machine Learning Methods Assessment for Denial of Service Detection in Wireless Sensor Networks. 2020 IEEE 6th World Forum on Internet of Things (WF-IoT); 2020. p. 1-6.

15. Al-Akhras M, Al-Issa AI, Alsahli MS, Alawairdhi M. POSTER: Feature Selection to Optimize DoS Detection in Wireless Sensor Networks. 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH); 2020. p. 263-265.

16. Al-issa AI, Al-Akhras M, ALsahli MS, Alawairdhi M. Using Machine Learning to Detect DoS Attacks in Wireless Sensor Networks. 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT); 2019. p. 107-112.

17. Premkumar M, Sundararajan TVP. DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks. Microprocessors and Microsystems. 2020;79:565-573.

18. Jinhui X, Yang T, Yao H. Intrusion Detection System for Hybrid DoS Attacks using Energy Trust in Wireless Sensor Networks. Procedia Computer Science. 2018;130:721-729.

19. Yang C, Liu F, Shen S, Qi J. An Energy-aware Approach with Spectrum Detection in Wireless Sensor Networks. 2021 IEEE 19th International Conference on Embedded and Ubiquitous Computing (EUC); 2021. p. 1-7.

20. Kurniawan MT, Yazid S. Mitigation and Detection Strategy of DoS Attack on Wireless Sensor Network Using Blocking Approach and Intrusion Detection System. 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE); 2020. p. 1-5.

## CONFLICTS OF INTEREST

None.

## FINANCING

None.

## AUTHORSHIP CONTRIBUTION

*Conceptualization:* Himani Sharma, Basheer Shajahan, Rajesh Elangovan, Manikandan Thirumalaisamy.
*Methodology:* Himani Sharma, Basheer Shajahan, Rajesh Elangovan, Manikandan Thirumalaisamy.
*Writing - Original Draft:* Himani Sharma, Basheer Shajahan, Rajesh Elangovan, Manikandan Thirumalaisamy.
*Writing - Review & Editing:* Himani Sharma, Basheer Shajahan, Rajesh Elangovan, Manikandan Thirumalaisamy.